通信情報保護學會誌
第7卷 第2號, 1997. 6

배달 및 내용 증명이 가능한 전자메일

Electronic Mail with Certification of Delivery and Contents

박 춘 식*

요 약

인터넷의 보급으로 인한 전자 메일의 증가가 급증하고 있다. 컴퓨터 통신망을 통해 주고 받는 전자 문서에 대해 문서의 내용과 그 문서가 배달되었음을 증명해주는 현행 우편제도하에서의 특수 우편물 취급 서비스가 그대로 적용될 수 있다. 본 고에서는, 이러한 서비스를 고려한 기존의 전자 우편 방식들을 조사 분석하여 정리하고자 한다. 분석된 자료들은 전자 우체국의 구현이나 실현을 위해 활용될 수 있으리라 생각된다.

1. 서 론

기업이나 개인의 사회 활동 가운데에서 중요한 역할을 차지하는 통신 수단으로써, 전자 메일을 이용하는 사람이 많이 늘어나고 있으며, 점차 보편화되고 있다. 일반적으로, 전화나 팩시밀리는 메시지를 통신 상대의 단말에 직접 보내는 데 반하여, 전자 메일은 상대의 메일 박스에 보내어 두면, 수신자가 메일 박스로부터 메시지를 가져가는 형태로 되어있다.

광역이나 국제적인 전자 메일을 구성하기 위해서는 표준화가필요한 데, 이러한 것은X.400이라는 권고로 MHS(Message Handling System)가 널리 오래 전부터 알려져있다. ISO에서도 이것을 표준으로 채택하여 개방형 구조인 OSI의 응용층의 하나로 추가하여 MOTIS(Message Oriented Text Interchange System)로 발표하였다.

또한 인터넷의 급속한 보급과 함께 전자 메일의 사용도 늘어나게 되어 TCP/IP 프로토콜을 이용하는 인터넷상에서의 전자 메일의 표준으로 RFC822이 채택되어 발표되었다. 그리고 전자 메일의 보호 서비스와 관련되어 PGP, PEM, MOSS 등의 용어들도 자주 등장하게 되었다.

최근, 미국에서는 전자 우편의 서류 발송 여부나 도착 시기, 수신자 신원 등의 법률적 문제를 해결한 전자 우편에 소인을 찍는, 즉, 전자 문서에 대해 송수신자 신분과 송수신 시각 등을 확인하고 문서가 제대로 배달되었음을 증명해주는 서비스를 '96년 3월경에 상용화

* 한국전자통신연구원

한다고 발표한바 있다[1]. 우리나라에서는 컴퓨터 전산망을 이용한 우편 배달이나 우체국의 정보 센터 기지화가 추진중이나 전자 우편에 대한 보호 서비스 그리고 기존 우편 제도에서 제공되고 있는 배달 및 증명 서비스는 고려되지 않는 것으로 알려지고 있다.

이에 본고에서는 정보보호기술연구의 원천기술연구와 관련하여, 문서의 내용과 그 문서가 배달되었음을 증명해주는 현행 우편제도하에서의 특수 우편물 취급 서비스를 고려한 기존의 전자 우편 방식들을 조사 분석하여 정리하고자 한다.

본 논문의 구성은, 2장에서는 본 고에서 사용될 용어의 정의와 관련 암호학적인 도구들에 대해서 언급하고자 한다. 3장에서는 기존의 직접 방식과 우체국을 이용하는 조정자 이용 방식에 대해서 살펴보고자 한다. 조정자를 이용하여 배달 및 내용 증명 서비스를 실현한 기존의 각종 방식에 대해서 4장에서 검토하여 보고, 마지막으로 결론 부분을 5장에서 언급하였다.

2. 준 비

2.1 정의

정의 1 [2] (배달증명) 수취인에게 우편물을 배달 또는 교부한 경우 그 사실을 배달 우체국에서증명하여 발송인에게 통지해주는 제도

배달 증명은 등기로 취급하는 우편물에 한하여 이용 가능하며, 발송시 발신자가 배달 증명을 청구하거나 필요시 사후에도 청구 가능하다. 배달 우체국은 수령증을 발신자에게 교부한다.

정의 2 [2] (내용증명) 발송인이 수취인에게 어떤 내용의 문서를 언제 발송하였다는사실을 우편관서가 공적으로 증명하는 제도

내용 증명은 우편물의 문서 내용을 후일의 증거로 남길 필요가 있을 경우 이용되는 제도로 우체국의 보관용, 수취인에게 보내는 원본 그리고 발송인 보관용 상호간에는 우체국의 도장으로 표시를 하며, 수취인이 수취를 거부할 경우가 있으므로 내용 증명이라는 표시를 우편물에는 하지 않는다. 배달 증명과 동일하게 발신자는 우체국으로 부터 수령증을 수령한다.

2.2 Cryptographic Tools

2.2.1 내용 은닉 서명 (blind signature)

일반적으로 서명자는 자신들이 서명할 메시지의 내용을 알고서 서명을 하게된다. 그러나, 경우에 따라서는 메시지의 내용을 보지 않은 채 서명을 받고 싶은 경우가 있다. 내용 은닉 서명은 메시지 내용은 상대방에게 알려주지 않으면서도 메시지에 대한 상대방의 서명을 얻게 되는 것으로 서명문과 메시지가 공개된 이후에도 서명자나 제3자에 의한 추적이 곤란한 서명으로 전자 현금이나 전자 선거등 프라이버시를 제공해야 하는 곳에 활용될 수 있다. 이곳에서의 개인의 프라이버시는, 전자 현금에서는 개인과 개인의 구매 사항의 관계를 알 수 없게 해주는 기능이며 전자 선거에서는 개인과 개인의 투표 내용과의 관계를 비밀로 해주는 기능을 말한다. 그리고 전자 현금인 경우 서명을 해주는 곳은 은행이며, 전자 선거인 경우는 선거 관리 위원회가 해당될 수 있다. 내용 은닉 서명을 이루기 위한 기본적인 요구조건은 다음과 같다.

- 메시지의 내용은 서명자에게는 은닉(blind)되어야 한다.
- 메시지와 서명문이 노출된 이후에도 메시지 소유자와 메시지와의 대응관계는 서명자에 의해 추적 불가능해야 한다.

내용 은닉 서명의 기본적 개념 제안[5]과 실현 방안[6]은 전자 현금에 활용하기 위해 D.Chaum에 의해 처음으로 제안되었다. 다음은 D.Chaum이 제안한 RSA 암호를 이용한 내용 은닉 서명[6]이다. 먼저, A가 서명자(signer) B에게 메시지 m을 은닉한 채 서명을 받고 싶다고 하고, B의 공개 키를 (e,n), 비밀 키를 d라고 한다.

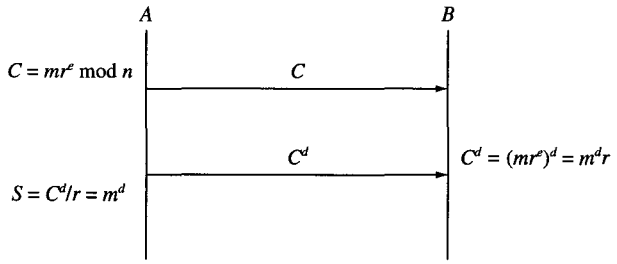


그림 1 RSA를 이용한 blind 서명 방식

(step 1) A는 난수 r를 생성하여 B에게 $C = mr^e \bmod n$을 계산하여 보낸다.

(step 2) B는 수신한 C에 대한 서명문 $C^d = (mr^e)^d \bmod n$을 계산하여 A에게 제시한다.

(step 3) A는 $S = C^d/r = m^d r^{ed}/r = m^d \bmod n$을 계산하여 B의 메시지 m에 대한 서명문으로 S를 얻게 된다.

2.2.2 복수 키 암호(multiple key cipher)

Multiple key cipher는 RSA 알고리즘의 확장형으로 키의 개수를 복수화하는 방식이다. 이를 간략히 요약하면 다음과 같다.

$$N = pq$$
$$e_1 \times e_2 \cdot \times e_k = 1 \bmod L \quad (1)$$

여기서, p와 q는 소수이며 $L = LCM(p-1, q-1)$이다. 식(1)에서 $e_1 \times e_2 \cdot \times e_{k-1}$은 랜덤수로 선택되며 e_k는 식(1)을 만족하는 값으로 선출되어야 한다.

$$E(E(E(M, e_1), e_2) \cdot \cdot \cdot), e_k)$$
$$= M^{e_1 \times e_2 \cdot \cdot \cdot \times e_k} \bmod N$$
$$= M^{r \times L+1} \bmod N$$
$$= M$$

Multiple key cipher는 이산 대수 문제인 DH 알고리즘에도 적용할 수 있으며[8]비밀 정보의 선택 분배, 다중 서명 방식 그리고 전자 선거에도 활용되고 있다[7], [8].

2.2.3 불확정 전송 프로토콜(oblivious transfer protocol)

Oblivious transfer protocol이란 다음과 같은 조건을 만족하는 프로토콜을 말한다.

- 수신자는 확률 1/2로 메시지 M을 얻게 된다.
- 수신자는 메시지 M을 얻었다는 것을 알 수가 있다.
- 송신자는 수신자가 메시지 M을 얻었는지 알 수가 없다.

RSA 암호를 이용한 1-out-of-2 Oblivious Transfer Protocol[11]에 대해서 소개한다(그림2)

본 프로토콜에서 송신자를 A, 수신자를 B라 하고 송신자 A의 공개 키를 (e,N) 그리고 비밀 키를 (d,N)이라 하며 송신자 S가 수신자 B에게 메시지 M_0 또는 M_1만을 보내고 싶다고 가정한다.

(step 1) A는 랜덤 수 $r_0, r_1(0 \le r_0, r_1 < N)$를 선택하여 $(e, N), r_0, r_1$를 B에게 전송한다.

(step 2) B는 랜덤 수 $l \in 0, 1$ 그리고 $K \in 0, 1, \cdots, N\text{-}1$를 선택하여

$$X = (K^e + r_l) \bmod N$$

를 A에게 보낸다.

(step 3) A는 $\hat{K}_i = (X - r_i)^d \bmod N, (i = 1, 0)$를 계산하고 $u \in 0, 1$를 랜덤하게 선택한 후 다음의 값들을 계산한다.

$$Y_0 = M_0 + \hat{K}_u \bmod N$$

$$Y_1 = M_1 + \hat{K}_{u\oplus 1} \bmod N$$

A는 Y_0, Y_1 그리고 u를 B에게 전송한다.

(step 4) K는 $\hat{K}_0$ 또는 $\hat{K}_1$의 값이므로 B는 다음 2식중에서 어느 한쪽을 올바르게 계산할 수가 있다.

$$M_0 = Y_0 - \hat{K}_0 \bmod N$$

$$M_1 = Y_1 - \hat{K}_1 \bmod N$$

그러나, A는 B가 M_0나 M_1중 어느 것을 취하였는 지를 알 수가 없다.

Oblivious Transfer Protocol은 비밀 정보의 교환, 계약 서명 그리고 전자 우편등 암호학적인 기본 도구로써 널리 활용되고 있다.

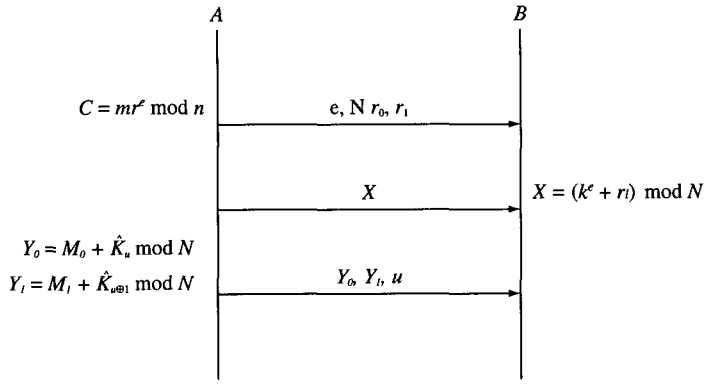


그림 2. RSA를 이용한 불확정 통신 프로토콜

2.2.4 bit commitment

Bit commitment 프로토콜은, 다음 2가지 단계로 구성된다.

· commit stage

A는 비트 b를 금고에 넣어 열쇠로 잠근 후, B에게 그 금고를 전해준다.

· revealing stage

A는 B에 금고의 열쇠를 전한다. B는 금고를 열어서 b를 취한다.

Bit commitment 프로토콜은 다음 2 조건을 만족하지 않으면 안된다.

- B는 $1/2 + 1/n^c$ 이상의 확률로 b를 추정하는 것은 불가능하다.
- A는 revealing stage에 있어서, b의 값을 바꾸는 것은 불가능하다.

일방향 치환이나 함수 그리고 영지식증명 등을 이용한 bit commitment 구성 방식들이 알려져 있다[9][10]

3. 전자메일에 의한 내용 및 배달 증명 서비스

3.1 직접 방식

UA(User Agent)가 MTA(Message Transfer Agent)를 경유하여 직접 다른 UA에게 메일을 전달하는 방식으로, Even 등에 의해 불확정 전송 프로토콜을 이용하여 제안된 방식이 문헌상에는 처음으로 나타나고 있으며, CCITT X.400 시리즈 그리고 EDI와 관련하여 많은 연구가 이루어지고 있는 방식이다. 직접 방식의 대표적인 모델은 MHS이며, 이러한 모델에 배달 증명 및 내용 증명 서비스를 제공하기 위한 시도가 많이 있어왔다. 내용 증명에 대한 프로토콜의 제안, 디지털 서명의 전자 우편에 적용[3] 불확정 전송 프로토콜을 이용하여 수령증과 암호키의 교환을 이루어 수신 증명을 제공하는 방안[4]등이 있다.

그러나, 이러한 방식들은 수신 증명 서비스를 제공하려고 할 경우, 공평한 관계가 이루어지지 못하며, 즉, 어느 한 쪽이 이익을 보게 되는 방식들로 이러한 한쪽만의 이익을 최소화하는 데 직접 방식의 한계가 있다.

3.2 조정자 이용 방식

직접 방식의 문제점을 해결하며 현행 우편 제도를 그대로 전자화 시키는 방식으로 우편 제도에서 제공되고 있는 서비스들을 제공하기 위한 연구들이 행하여 지고 있다. Nakao에 의한 방안[12]이 문헌상 최초로 보이며, 최근에 이 분야에의 연구[17][18][19][20]가 활발한 편이다.

이 방안은 수신자와 송신자사이에 모든 참가자가 신뢰할 수 있는 제3의 조정자(경우에 따라서는 전자 우체국)를 선정하여 모든 전자 우편이 이를 통하여 행하여 지는 것으로 직접 방식에서의 문제점을 근본적으로 해결할 수 있다. 그러나, 조정자가 필요하므로 이로 인한 프로토콜의 증가와 실질적인 활용시의 고려사항이 증가하게 된다.

4. 내용 및 배달 증명이 가능한 전자 우편 방식

현행의 우편 시스템에서 실시되고 있는 특수 서비스중에서 내용 증명, 배달 증명을 전자 우편상에서 실현하기 위한 연구가 진행중이다. 내용 증명은 언제, 누가, 누구에게, 어떠한 내용의 문서를 송신하였는가를 후일 증명하는 것이고, 배달 증명은 수신자까지 문서가 도달했음을 증명하는 것이다. 이 두가지의 서비스는 통상 조합하여 이용된다.

4.1 Nakao 방식[12]

Nakao는 현행의 내용 증명, 배달 증명의 순서를 전자 우편상에서의 실현 가능한 시스템으로 제안하였다. 우편의 송신은 신용할 수 있는 조정자를 두고 행하였으며, 기본적인 순서는 그림 3에 나타내었다.

(step 1) 송신자는 자기의 비밀 키 K_{SA}로 메일에 디지털 서명을 하여 조정자에게 보낸다.

(step 2) 조정자는 서명 C를 공개 키 K_{PA}로 암호화하여 그 결과 얻어진 M의 형식 검사를 한다. 또, 조정자 고유의 Hash 함수 h로 인증자 h(c)를 작성하여 그것을 내용 증명 수락 번호 n과 쌍으로 써 보관한다. 조정자는 n과 n을 조정자의 비밀 키 K_{SI}로 디지털 서명한 것을 송신자에게 보낸다. 송신자는 n의 서명을 검사한 후 $(n, D_{KSI}(n), D_{KSA}(M))$을 보낸다.

(step 3) 수신자의 정당성을 PIN등으로 확인한 조정자는 수신자의 우편을 읽어내라는 요구에 따라 우편을 송신한다. 이것으로 배달이 완료되었다고 보고 배달 증명 통지를 송신자에게 보낸다.

(step 4) 내용 증명이 필요할 때 송신자는 $(n, D_{KSI}(n), D_{KSA}(M))$을 조정자에게 보낸다. 조정자는 $n = E_{KPI}(D_{KSI}(n))$이 성립함을 확인하고, 또 n을 이용하여 데이타 베이스중의 인증자 h(c)을 끌어낸다. 이것과 $D_{KSA}(M)$을 해쉬 처리하여 얻어진 인증자가 일치하면 내용 증명을 송신자에게 준다.

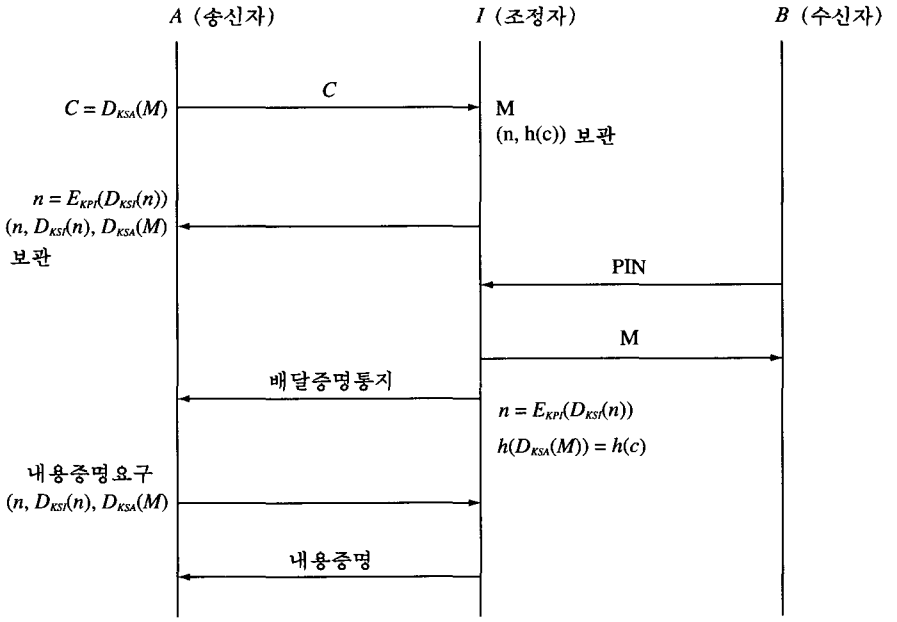


그림 3. Nakao 방식

4.2 TUA(Tanaka, Uchida and Akiyama)방식[13]

이 방식은 수신자가 수령한 암호문의 전문에 디지털 서명을 한 후에야만 조정자로 부터의 복호화 키를 받아서 전문의 내용을 알 수 있는 수령증 제시후 개봉 가능 방식이다. 기본 원리는 그림4 와 같다. 먼저, 송신자를 S, 수신자를 R 그리고 조정자를 A라 하고, 공개키 암호 방식의 공개키 및 비밀키를 E_S, E_R, E_A 그리고 D_S, D_R, D_A 로 한다.

(step 1) 송신자는 메세지 M을 수신자의 공개

키 E_R을 이용하여 암호화하고, 이 결과를 다시 자신의 비밀키 D_S로 서명한 내용 $C_1(= D_S(E_R(M)))$을 조정자 A에게 보낸다.

(step 2) 조정자는 C_1을 수신자가 알지 못하는 암호화 키 K_{AR}를 이용하여 비밀키 암호 방식으로 암호화 한 후, 수신자에게 $C_2(= K_{AR}(C_1))$을 전송한다. 이 단계에서, 수신자는 비밀키 K_{AR}를 알지 못하므로 메시지를 읽어볼 수가 없으므로 개봉을 하지 못하는 형태가 되며 송신자가 누구인지도 알지 못하게 된다.

(step 3) 수신자는 암호문 C_2를 자신의 비밀키 D_R로 디지털 서명한 값 $C_3(= D_R(C_2))$를 조정자 A에게 보낸다. 결국 C_3가 수신자의 수령증에 해당하게 된다.

(step 4) 조정자 A는 수신자의 수령증을 확인한 후, C_1의 암호화에 사용되었던 암호화 키 K_{AR}을 수신자에게 전송한다.

(step 5) 수신자는 이 키로 메세지의 내용을 알 수 있으며, 조정자는 이 키와 수신자로 부터의 수령증 C_3를 송신자에게 보냄으로써, 송신자는 이들을 송신한 메세지 M과 함께 보관함으로써 이들이 내용증명 및 배달 증명서의 역할을 하게 된다.

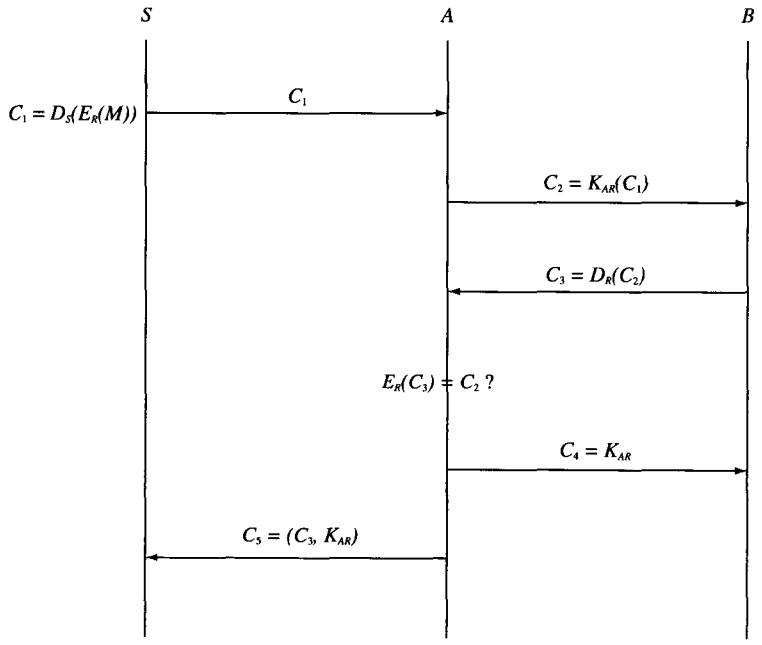


그림 4 TUA 방식

4.3 OWK(Oginao, Wakasugi and Kasahara)방식[14]

비밀키 방식과 공개키 방식 모두를 사용하는 TUA방식을 공개키 방식만으로 가능하게 한 방식으로 RSA 암호와 ElGamal 암호를 이용한 두가지 방식을 제한 하고 있다. RSA암호를 이용한 OWK방식을 그림5에 나타내었으며, 기본 동작은 다음과 같다.

(step 1) 송신자는 메세지 M을 수신자의 공개키 E_R을 이용하여 암호화하고, 이 결과를 다시 자신의 비밀키 D_S로 서명한 내용 $C_1(= D_S(E_R(M)))$을 조정자 A에게 보낸다.

(step 2) 조정자는 C_1을 자신의 비밀키 D_A로 서명한 내용 $C_2(= D_A(C_1))$을 수신자에게 메일의 송신자가 S라는 사실과 함께 전송한다.

(step 3) 수신자는 암호문 C_2를 조정자의 공개키 E_{A1}로 암호하고 그 결과를 자신의 비밀키 D_R로 디지틀 서명한 값 $C_3(= D_R(E_{A1}(C_2)))$를 조정자 A에게 보낸다. 결국 C_3가 수신자의 수령증에 해당하게 된다.

(step 4) 조정자 A는 수신자의 수령증을 확인한 후$(E_R(C_3) \stackrel{?}{=} E_{A1}(D_A(C_1)))$, E_{A2}는 수신자에게 그리고 C_3와 E_{A2}는 송신자에게 전송한다.

(step 5) 수신자는 E_{A1}과 E_{A2}를 이용하여 C_2를 복호하여 송신자가 보낸 C_1를 계산한다. 이 C_1으로 부터 송신자의 서명을 확인하고 메일의 내용을 수신자의 비밀키 D_R를 이용하여 복호할 수 있다. 송신자는 C_3와 E_{A2}를 이용하여 송신자가 보낸 C_1과 일치하는 지를 확인한 후 이들을 송신한 메세지 M과 함께 보관함으로써 이들이 내용증명 및 배달 증명서의 역할을 하게 된다.

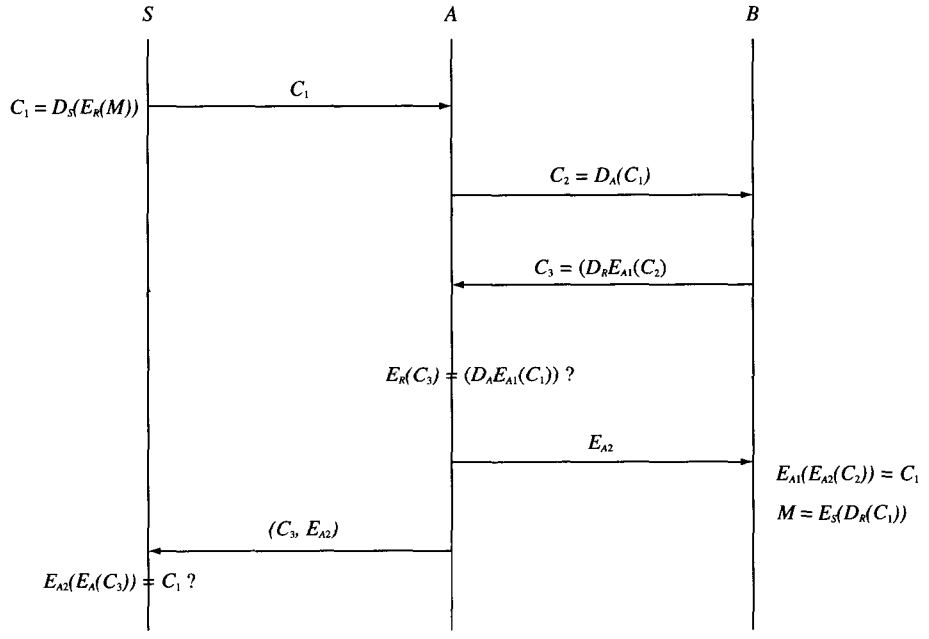


그림 5. OWK 방식

그러나 OWK 방식은 다음과 같은 문제점들을 내포하고 있다.

- 수신자가 특정 메일만을 거부하는 것은 곤란하나 특정 송신자를 거부할 수는 있다.
- 조정자가 사용하는 E_{I1}과 E_{I2}는 1회밖에 사용할 수 없다. 즉, 조정자의 공개키는 매회 변경되어야 하므로 실용적이지 못하다.

4.4 BT(Bahreman and Tygar) 방식[15]

OWK 방식과 유사한 방식으로 메시지 보호 방식으로는 비밀키 암호 방식을, 그리고 디지털 서명으로써는 공개키 암호 방식을 별도로 1994년에 제안하였다. 특별히 새로운 개념은 없으며 OWK 방식에 대한 정보를 알지 못하였기 때문에 제안된 것으로 이를 그림 6에 나타내었으며, 기본 동작은 다음과 같다.

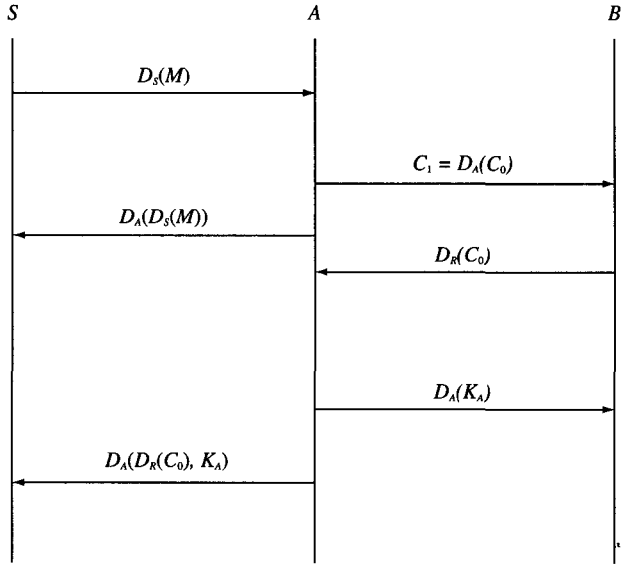


그림 6. BT방식

(step 1) 송신자는 메세지 M을 자신의 비밀키 D_S을 이용하여 계산한 즉, 자신의 비밀 키 D_S로 서명한 내용 $CEM(=D_S(M))$을 조정자 A에게 보낸다.

(step 2) 조정자는 CEM을 비밀키 암호 방식용 비밀키 K_A를 이용하여 암호화된 $C_0(=(CEM, K_A))$를 먼저 발생한다. 이 C_0를 조정자 자신의 공개키 암호용 비밀키 D_A를 이용하여 서명한 결과인, $C_1(=D_A(C_0))$를 수신자 R에게 전송한다. 한편, 송신자에게서 수령한 CEM에 대한 제출 증거로서, 조정자가 서명한 내용, $D_A(CEM)$를 송신자에게 보낸다.

(step 3) 수신자는 암호문 C_1을 조정자의 공개키 E_A로 암호하고 그 결과 C_0를 자신의 비밀 키 D_R로 디지털 서명한 값 $C_2(=D_R(E_A(C_1))$를 조정자 A에게 수령증으로서 보낸다.

(step 4) 조정자 A는 수신자의 수령증을 확인한 후($E_R(C_2) \stackrel{?}{=} C_0$), $D_A(K_A)$는 수신자에게 그리고 $D_A(C_2, K_A)$는 송신자에게 전송한다.

(step 5) 수신자는 K_A를 이용하여 C_0를 복호(비밀키 암호 방식)하여 송신자가 보낸 *CEM*을 계산한다. 이 *CEM*으로 부터 송신자의 서명을 확인하고 메일의 내용을 송신자의 공개키 E_S를 이용하여 복호할 수 있다. 송신자는 C_2와 K_A를 송신한 메세지 M과 함께 보관함으로써 이들이 내용 증명 및 배달 증명서의 역할을 하도록 한다.

4.5 ZG(Zhou and Gollmann) 방식[16]

전자 우편에 있어서 부인 봉쇄 기능은 아주 좋은 역할을 하게 된다. 특히 수령증과 메시지와의 교환시에는 공평한 교환이 이루어지는 것이 전자 우편에서는 무엇보다도 중요하다. 이러한 관점에서 공평한 부인 봉쇄 프로토콜(Fair Non-repudation Protocol)을 개발하여 전자 우편에 적용하였다. 가장 최근('96)에 제안된 방식을 그림 7에 나타내었으며, 기본 동작은 다음과 같다.

(step 1) 송신자는 메세지 M을 비밀키 암호용 비밀키 K_S을 이용하여 암호화한 암호문 C_0(= (K_S, M))와 자신의 비밀키 D_S로 서명한 내용 NRO(= $D_S(C_0)$)을 수신자 R에게 보낸다.

(step 2) 수신자는 수신한 C_0에 대해서, 자신의 비밀 키 D_R로 서명한 내용 NRR(= $D_R(C_0)$)을 송신자 S에게 보낸다.

(step 3) 송신자는 암호문 C_0의 암호키로 사용된 K_S와 K_S를 자신의 비밀 키 D_S로 디지털 서명한 값 C_1(= $D_S(K_S)$)를 조정자 A에게 제시한다.

(step 4) 조정자 A는 수신한 K_S를 이용하여 자신의 공개키 암호용 비밀키 D_A로 서명한 내용 C_2(= $D_A(K_S)$)와 K_S를 송

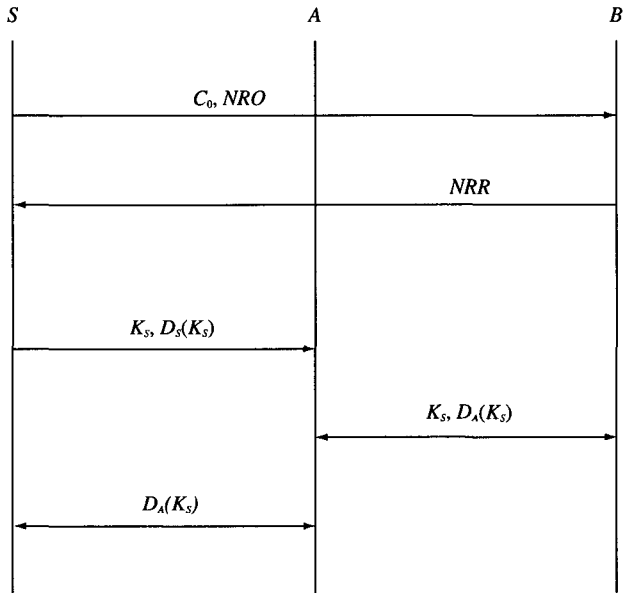


그림 7. ZG 방식

수신자가 악세스할 수 있는 디렉토리에 게시한다.

(step 5) 수신자는 디렉토리로부터의 K_S를 이용하여 C_0를 복호하여 송신자가 보낸 메시지 M을 계산한다. 송신자는 분쟁시의 증거로서, C_2를 저장하여 둔다.

5. 결 론

본 고에서는 조정자를 이용한 안전한 전자우편에 대하여 기존에 제안된 방식들을 중심으로 살펴보았다. 수령증과 메시지를 안전하고 공평하게 교환하는 방식들은 현행 우편 방식에서 제공되는 우편 서비스를 전자화하여 제공하는 것으로 내용증명, 배달증명에 대한 서비스를 전자화하여 제공할 수 있음을 알 수 있었다. 이러한 방식들은 기존의 우체국의 업무를 전자화하는 데 크게 기여할 것이며, 암호의 응용 분야로써 활용되리라 생각된다.

참 고 문 헌

[1] 조선일보, 전자우편에도 소인찍는다. 1995.4.23.

[2] 정보통신부, 우편업무편람, 제4장 우편물의 특수 취급, 1994.

[3] D.W.Davis,"Applying the RSA Digital Signature to Electronic Mail", IEEE, Computer, pp. 55--62,1983.

[4] S.Even, O.Goldreich and A.Lempel, "A Randomized Protocol for Signing Contracts", Comm. of ACM, Vol.28, No.6, pp.637 -647, 1985.

[5] D.Chaum,"Blind Signatures for Untraceable Payments", Advances in Cryptology, Proceedings of Crypto' 82, Plenum Press, pp.199-203, 1983.

[6] D.Chaum,"Security Without Identification : Transaction Systems to Make Big Brother Obsolete", Communications of the ACM, Vol.28, No.10, pp.1030-1044, 1985.

[7] C.A.Boyd, "Some Applications of Multiple Key Ciphers", Advances in Cryptology, Proceedings of EUROCRYPT '88, Springer-Verlag, pp.455-467, 1988.

[8] C.A.Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme", Advances in Cryptology, Proceedings of EUROCRYPT' 89, Springer-Verlag, pp.617-625, 1989.

[9] I.Damgard, "On the existence of bit commitment schemes and zero knowledge proofs", Advances in Cryptology, Proceedings of Crypto' 89, pp.17--27, 1989.

[10] M.Noar, "Bit commitment using pseudo randomness", Advances in Cryptology, Proceedings of Crypto' 89, pp.128-136, 1989.

[11] K.Kurasawa and S.Kaito, "Non-Interactive 1-out-of-n Oblivious Transfer and 3 move ZKIP", Technical Report of IEICE, ISEC 90-4, pp.21-27, 1990.(in Japanese)

[12] K.Nakao, "Applying Cryptography to Contents-certified Service", The 2nd CIS Kenkyukai,1985.(in Japanese)

[13] Y.Tanaka, T.Uchida and M.Akiyama, "Contents and Delivery Certification Service Using Cryptography in Elec-tronic Mail",IEICE of Japan, shinkakuron, Vol.J70-D, No.2, pp.423-431,1987.(in Japanese)

[14] K.Ogino, K.Wakasugi and M.Kasahara, "A Scheme of the Security System for Electronic Mail or Bond Ticket", Technical Report of IEICE, ISEC 91-13, pp.33--37, 1991.(in Japanese)

[15] A.Bahreman and J.D.Tygar, "Certified Electronic Mail", Proc. of the Internet Society Symposium on Network and Distributed System Security, pp.3-19, 1994.

[16] J.Zhou and D. Gollmann, "A Fair Non-repudation Protocol", Proc. of the 1996 IEEE Symposium on Security and Privacy, pp.55-61, 1996.

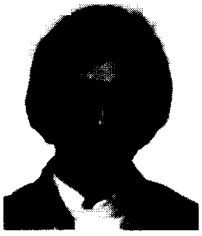
[17] K.Ogino, K. Wakasugi and M. Kasahara, "A Study on Electronic mail Certification based on RSA Cryptosystem", Technical Report of IEICE, ISEC 92-69, pp.47--53, 1993.(in Japanese)

[18] A.Adachi and T.Sugimura, "A Consideration on Certification Systems for Delivery and Contents in Electronic Mail", Technical Report of IEICE, ISEC93-16, pp.1-6, 1993.(in Japanese)

[19] S.Houmura, R.Sakai and M. Kasahara, "A Note on Electronic mail with Certification of Delivery and Contents", Technical Report of IEICE, ISEC94-56, pp.45-49, 1995.(in Japanese)

[20] J.Zhou and D. Gollmann, "Observations on Non-repudation", Advances in Cryptology, Proceedings of ASIACRYPT' 96, Springer-Verlag, pp.133-144, 1996.

□ 著者紹介



박 춘 식

광운대학교 전자통신과 졸업(학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 ~ 현재 한국전자통신연구원 책임연구원
저서 : 전자상거래, 이한출판사, 1997년
한국통신정보보호학회 편집이사

※ 주관심 분야 : 암호이론, 정보이론, 통신이론